UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

-v-

ANDREY KOSTIN et al.,

Defendants.

Case No. 1:24-cr-00091 (GHW)

DECLARATION OF MICHAEL SUCCI IN SUPPORT OF MOTION TO SUPPRESS DEVICE PASSCODE AND RELATED FRUITS

Pursuant to 28 U.S.C. § 1746, I, Michael Succi, declare under oath as follows:

1. I am the founder of Succi Investigative Services, a forensic examination and investigation firm in San Juan Capistrano, California. I have been in this position since May 2022.
2. From April 1999 to April 2022, I served as a Special Agent with the United States Secret Service ("USSS"). From October 1995 to April 1999, I was a member of FBI's Special Surveillance Group. A copy of my resume is attached as Exhibit A.
3. While serving with the USSS, I was a member of the Electronic Crimes Task Force and Digital Forensics Laboratory in the Los Angeles Field Office. I conducted cyber investigations and digital forensics examinations for federal, state, and local investigators.
4. I have extensive experience with Graykey, a forensic tool used by law enforcement to extract data from cell phones. I personally performed or supervised approximately 100 iPhone extractions using Graykey while working for the USSS. I have also kept abreast of developments to Graykey since leaving government service.

5. Defendant Vadim Wolfson retained me to opine on declarations submitted by Special Agent John Gomez (ECF No. 93-16) and Investigative Analyst Enrique Santos (ECF No. 93-17). In addition to those declarations, I have reviewed portions of the government's document production to counsel for Mr. Wolfson related to data extracted by Graykey from Mr. Wolfson's iPhone 15 (WOLFSON_00000274), as well as technical reports that the government produced in this matter (WOLFSON_00000339 – WOLFSON_00000346). I understand that FBI conducted the Graykey extraction using a passcode that Mr. Wolfson provided to agents on the morning of his arrest in Austin, Texas. This passcode was used in lieu of a Graykey After First Unlock ("AFU") extraction because an extraction with the passcode obtains more information from the device. The passcode was also used to manually obtain saved usernames and passwords from third-party applications and other web-based accounts on the device that otherwise would not have been obtained with an AFU extraction.

6. I disagree with the assertions of Special Agent Gomez and Investigative Analyst Santos that they can be "virtually certain" of a successful Graykey extraction, without using a passcode, of all data contained in an iPhone other than "emails, recently visited locations, and iOS Health application data." Having personally observed many instances where Graykey was unsuccessful in obtaining any data during iPhone extractions, or where the result of the extraction was significantly less data than the three categories identified above, I would not be comfortable expressing anywhere near this level of confidence without having actually attempted to use Graykey on the particular device in question without the benefit of a passcode.

7. In this matter, my understanding is that FBI never tried using Graykey on Mr. Wolfson's iPhone without first inputting his passcode. The fact that Graykey was successful in extracting data after an FBI analyst inputted Mr. Wolfson's passcode into the iPhone at issue says nothing more generally about FBI's ability to reliably extract data from that iPhone had FBI analysts not inputted the passcode into the iPhone and instead relied solely on the Graykey to attempt a data extraction.

8. Based on my review of the Gomez and Santos declarations and the data and reports referenced above in Paragraph 5 of this declaration, I am unable to discern the basis for the statements in the declarations that FBI necessarily would have been able to conduct an AFU extract, as opposed to a Before First Unlock ("BFU") extract. I have seen no evidence confirming that Mr. Wolfson's iPhone was in an AFU state at the time of seizure by FBI. I can conclude that the iPhone was most likely in a BFU state at the time of the extraction on May 23, 2024, due to the manner in which FBI processed and transported the iPhone.

9. For iPhones that are in a BFU state, the data that can be extracted using Graykey is extremely limited. Examples of such data include voicemail, partial media, system metadata, partial application data, and account data.

10. I have personally observed many instances of iPhones that were seized in a BFU state or that were in a BFU state at the time of extraction.

11. Phones can be in a BFU state in a number of situations, including following software updates, after someone powers off a device, or when someone plugs a dead device into an outlet and does not enter a passcode prior to the device's seizure. These are not hypothetical situations—law enforcement encounters with BFU phones frequently arise in everyday investigations, and I see no basis in this matter to assume that the iPhone in

question was necessarily in the AFU state when it was seized on the morning of Mr. Wolfson's arrest.

12. I have also reviewed a photograph (WOLFSON_00000347) of a sealed government evidence bag that appears to show how Mr. Wolfson's phone was stored in a manilla envelope, and disconnected from a power source, between February 29, 2024, and May 23, 2024. Under such circumstances, the iPhone undoubtedly would have powered off when its battery died after a short time period, ensuring that the iPhone would have been in a BFU state upon being rebooted subsequently by an FBI analyst at a later date.

13. Even in the case of successful AFU extractions, the results for certain applications can vary significantly. For instance, I have personally observed instances where numerous third-party applications, including WhatsApp messages, cannot be fully retrieved during an otherwise routine AFU extraction using Graykey. Manually obtaining the usernames and passwords for third-party applications increases the likelihood of successfully having access to all third-party applications on the device, including messaging, financial, and other private and secure applications. In my experience, Graykey has the ability to locate and extract passwords on the device but is rarely successful in obtaining usernames and passwords for most third-party applications.

14. In my experience working in law enforcement, the standard operating procedure when dealing with seized phones is to put them into airplane mode—*i.e.*, turn off the phone's wireless transmission functions—upon seizure. Not doing so creates a substantial risk that future access to the iPhone in question will be limited by events that could include, but are not limited to, software updates that can cause phones to reboot and go into a BFU state and remote wiping. I was surprised to learn from FBI's technical reports that the iPhone

in this case was not in airplane mode. This fact increases even further my level of disagreement with the claims from the government's declarants that they can be "virtually certain" that the government could have conducted an effective AFU extraction of Mr. Wolfson's iPhone 15 using Graykey.

15. I am personally familiar with FBI's significant backlog for analyzing seized phones. Based on my experience with law enforcement triaging practices, I have no confidence that Mr. Wolfson's iPhone 15 would have been analyzed immediately after the September 2024 Graykey update if it had not previously been accessed using the passcode. Even setting aside the backlog issue, which, in my experience, can create significant delays in obtaining Graykey extractions, agents do not uniformly submit previously seized devices for new analysis when Graykey updates become available. Given these considerations, at least several months, and possibly much more time, could have passed before FBI attempted a Graykey extraction on Mr. Wolfson's iPhone 15.

16. I have also reviewed the declaration of Special Agent Roland Chattaway (ECF No. 93-15), and in particular the following statement at Paragraph 4: "At the time of Wolfson's arrest, I believed that asking Wolfson about his phone passcode was a permissible, non-substantive area of inquiry that did not require *Mirandizing* him, akin to asking about his pedigree information, such as his name or date of birth." This statement is not consistent with my experience with FBI or as a law enforcement agent more generally. Seizures of iPhones are extremely common occurrences in law enforcement investigations, and FBI personnel are well trained on the relevant legal requirements and the handling of digital evidence, both as a matter of basic education and in preparatory briefings prior to the execution of search warrants.

I declare under penalty of perjury that the foregoing is true and correct.

Dated: January 10, 2025
San Juan Capistrano, CA

Michael Succi

EXHIBIT A

MICHAEL SUCCI

Email: Mike@SucciInvestigations.com
Cell: 657/244-9334

33959 Doheny Park Road #1007
San Juan Capistrano, CA, 92675

EXPERIENCE

CEO / Founder : Succi Investigative Services — May 2022 - Present

Created a private investigations and digital forensics company that provides assistance to criminal and civil litigations. Utilizes UltraKit, Writeblocker, FTK imager, Cellebrite and Magnet Axiom Forensic Software to conduct digital forensic examinations. Assists in investigations, to include surveillances, background checks, social media preservation, criminal history inquiries, report writing and trial preparation. Conducting advance protection assignments for early presidential candidates, congressional election fundraisers, rally's and other large speaking events.

United States Secret Service - Special Agent : April 1999 - April 2022

Conducted investigations of counterfeit currency, credit card fraud, identify theft, credit card skimming and various other white-collar crimes. Testified in federal grand jury, applied for and received search warrants, arrest warrants and seizure warrants, executed search warrants, executed arrest warrants, and participated as the case agent in federal and state trials.

Was a member of the USSS Presidential Protective Division at the White House under the Bush and Obama Administrations. Conducted daily shift work, protection advances and White House Access Control for the presidential detail and complex. During this time period, I conducted numerous foreign and domestic advances, including the lead advance for the president's trip to Rome, Italy. These advances included being the site agent for airports, major events and summits as well as smaller events, such as embassy meet and greets and presidential dinners with hosting countries. I was also the foreign logistics agent and field office counterpart for presidential foreign visits. As an advance special agent, I created and enforced the security plan, which included providing a perimeter and interior layer of security for fixed and roving posts, motion and heat sensors, radiation sensors, searches for planted bugs and recording devices, plans for egress and evacuation, crowd control, public/VIP and media access, fire and public safety plans, camera installations and limiting access to other cyber related systems, including water, heating, HVAC and power. These security plans also included presidential buffers, arrival and departure areas, plans and responses for chemical and biological weapons, plans for protestors and fence jumpers and security from aircraft and drones. Negotiated with

White House Staff and host committee on security measures and balanced the security budget for the overall trip and each protective site.

Was a member of the Electronic Crimes Task Force and Digital Forensics Laboratory in the Los Angeles Field Office. Conducted cyber investigations and digital forensic examinations for federal, state and local investigators. Testified in federal and state court as an Expert Witness in the field of digital forensics. Received training in and utilized the following forensic software:

- Magnet Axiom
- GrayKey
- Cellebrite Premium
- Forensic Toolkit (FTK)
- Forensic Explorer (FEX)
- Encase
- Cellebrite
- Berla Vehicle Forensics

Federal Bureau of Investigation (FBI) - October 1995 - April 1999

Was a member of the Special Surveillance Group. This group was trained in vehicle and foot surveillance as well as disguises and undercover operations. Assisted in investigations involving espionage and domestic and international terrorism.

EDUCATION

University of California, Irvine — BS Sociology (Criminology and Law) - 1995

Including two (2) years as a Computer Science Major